



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.  | CONFIRMATION NO. |
|-----------------|-------------|----------------------|----------------------|------------------|
| 09/735,087      | 12/11/2000  | David Michael Kurn   | 20206-033 (P00-3017) | 5325             |

7590

07/01/2005

Hewlett-Packard Company  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER

SON, LINH L D

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2135

DATE MAILED: 07/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/735,087

Applicant(s)

KURN ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 11 December 2000.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-12, 14-27 and 29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12, 14-27 and 29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 04/01
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This Office Action is responding to the Amendment received on 04/22/05.
2. Claims 1, 3, 16 are amended. Claims 13 and 28 are canceled.
3. Claims 1-12, 14-27, and 29 are pending.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-44 are rejected under 35 U.S.C. 102(b) as being anticipated by Brennan et al, US Patent No. 5675649, hereinafter "Brennan".

6. As per claims 1 and 16, Brennan teaches "A cryptographic system in a computer system, comprising: a database, the database configured to contain sensitive information; at-least a key repository process operating in the computer system" in (Col 1 lines 10-27); "two or more master keys of which at least one master key is a most-secure master key and requiring a multi-part construction to be exposed, the multi-part construction requiring information from at least two most-secure key owners for the most-secure key to be exposed" in (Col 5 lines 27-35, Col 13 lines 45-55, Master key), "the most-secure master key providing protection to the sensitive information" in (Col 1 lines 20-28, and Col 9 lines 5-40), "relative to the at least one most-secure

Art Unit: 2135

master key each of the remaining one or more master keys is a less-secure master key and requiring construction from fewer parts to be exposed” in (Col 9 lines 45-63), “the at least one most-secure master key can be used for detecting tampering of any less secure master key” in (Col 9 lines 45-63); and “means for cryptographically linking one or more of the at least one most secure master key with one or more less-secure master keys such that any tampering of the one or more less-secure master keys can be detected” in (Col 14 lines 10-30) .

7. As per claims 2 and 17, Brennan teaches “A cryptographic system as in claims 1 and 16, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with the one or more less-secure master keys, and saving the result in the database” in (Col 14 lines 10-30, and Col 18 lines 10-30).

8. As per claims 3 and 18, Brennan teaches “A cryptographic system as in claims 1 and 16, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with a random value and further concatenated with the one or more less-secure master keys, and saving the result in the database” in (Col 14 lines 10-30, and Col 18 lines 10-30).

9. As per claims 4 and 19, Brennan teaches “A cryptographic system as in claims 3 and 19, wherein the random value is a Salt” in (Col 16 lines 48-58).

10. As per claims 5 and 20, Brennan teaches "A cryptographic system as in claims 1 and 16, wherein for each of the one or more most-secure master keys the cryptographic linking is performed by using that most-secure master key as a symmetric encryption key, to compute a symmetric message authentication code, and retaining some or all of the result" in (Col 21 lines 15-28, and Col 18 lines 10-30).

11. As per claims 6 and 21, Brennan teaches "A cryptographic system as in claims 1 and 16, wherein for each of the one or more most-secure master keys the cryptographic linking is performed to produce an 8-byte result by using that most-secure master key as a symmetric encryption key, to compute a symmetric message authentication code, and retaining a 4-byte portion of the result" in (Col 21 lines 15-28, and Col 18 lines 10-30).

12. As per claims 7 and 22, Brennan teaches "A cryptographic system as in claims 6 and 16, wherein the symmetric message authentication code computed using cipher-block chaining (CBC) method of any symmetric encryption algorithm" in (Col 21 lines 15-28, and Col 18 lines 10-30).

13. As per claims 8 and 23, Brennan teaches "A cryptographic system as in claims 7 and 16, wherein the CBC is performed using a random number as an initialization

Art Unit: 2135

vector, and wherein the initialization vector is saved along with the result” in (Col 16 lines 48-58, Col 21 lines 15-28, and Col 18 lines 10-30).

14. As per claims 9 and 24, Brennan teaches “A cryptographic system as in claims 1 and 16, wherein the two or more master keys are kept in non-swappable physical memory” in (Col 5 lines 35-45).

15. As per claims 10 and 25, Brennan teaches “A cryptographic system as in claims 9 and 23, wherein the non-swappable physical memory is protected” in (Col 5 lines 35-45).

16. As per claims 11 and 26, Brennan teaches “A cryptographic system as in claims 1 and 16, wherein the two or more master keys are kept in virtual memory” in (Col 5 lines 35-45).

17. As per claims 12 and 27, Brennan teaches “A cryptographic system as in claims 1 and 16, wherein, respectively, the at least one most-secure master key and the one or more less-secure master keys, include a protection key and an integrity key, the protection key protecting access to sensitive information and the integrity key ensuring the integrity of the sensitive information” in (Col 21 lines 15-35).

Art Unit: 2135

18. As per claims 14 and 29, Brennan teaches "A cryptographic system as in claims 1 and 16, wherein the sensitive information can be a public key" in (Col 21 lines 15-35).

19. As per claims 15, Brennan teaches "A cryptographic system as in claim 1, wherein the means for cryptographically linking is a key repository process for enforcing enterprise policies and policy decisions" in (Col 21 lines 15-35).

### ***Double Patenting***

20. The non-statutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

21. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

22. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

23. Claims 1-12, 14-27, and 29 of the instant application No. 09735087, hereinafter '087, are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-44 of copending Application No. 09736718, hereinafter '718. Although the conflicting claims are not identical, they are not patentably distinct from each other because as follow:

24. The instant application '087:

Exemplary Claim 1 recites:

- (1) A cryptographic system in a computer system, comprising: a database, the database configured to contain sensitive information; at-least a key repository process operating in the computer s System;
- (2) two or more master keys of which at least one master key is a most-secure master key and requiring a multi-part construction to be exposed,
- (5) the multi-part construction requiring information from at least two most-secure key owners for the most-secure key to be exposed,



Art Unit: 2135

(3) the most-secure master key providing protection to the sensitive information,

(6) relative to the at least one most-secure master key each of the remaining one or more master keys is a less-secure master key and requiring construction from fewer parts to be exposed, the at least one most-secure master key can be used for detecting tampering of any less secure master key;

(7) and means for cryptographically linking one or more of the at least one most secure master key with one or more less-secure master keys such that any tampering of the one or more less-secure master keys can be detected.

25. The copending application '718:

Exemplary Claim 1 recites:

(1) A cryptographic system in a computer system, said cryptographic system comprising: at least one server; a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server; a key repository process on one of said at least one server,

(2) said key repository having two master keys,

- (3) said two master keys constructed and arranged to manage information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database;
- (4) at least one operator, said at least one operator having access to a first of said master keys;
- (5) and the at least two owners, each of said owners having a portion of a second of said master keys; wherein said at least operator and at least one of said owners are required to start said key repository process"

26. As underlined above, the limitation **(1)** of both applications recites the exact language.

However, the limitations **(2)**, **(3)**, and **(5)** in '087 claim the two master keys, a method of implementing the two master keys in the invention, and further construction of the master keys. The limitations **(2)**, **(3)**, and **(5)** in '718 only claim the master keys, and a method of implementing the master keys in the invention. It is clearly that the limitations **(2)**, **(3)**, and **(5)** in instant application '087 are more specific comparing to the limitation **(2)**, **(3)**, and **(5)** in the copending application '718, which are more generic. Further, the limitations **(6)** and **(7)** in '087 are not in '718. Nonetheless, those limitations **(6)** and **(7)** further claim the detail construction of the master keys. Therefore, it is clearly that the exemplary claims 1 in '087 anticipate exemplary claim 1 in '718.

Art Unit: 2135

27. Exemplary Claim 1 in '087 are generic to the species of claims 1 and 38 in '718. Thus, the generic invention is "anticipated" by the species of the copending application invention. Cf., *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In *re Van Ornum*, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); *Schneller*, 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting."  
*(In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).*

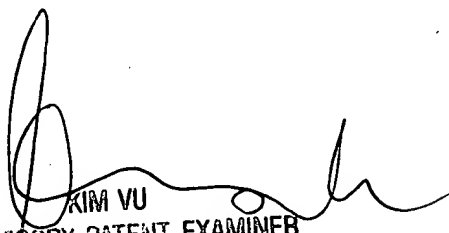
28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Patent Examiner



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100